Discrete Mathematics 96 (1991) 111–129
North-Holland

Inclusion transformations: (n, m)-graphs and their classification

R.E. Peile

Communication Sciences Institute, Department of Electrical Engineering Systems, University of Southern California, University Park, Los Angeles, CA 90089-0272, USA

Received 4 March 1988
Revised 13 December 1989

Abstract

Peile, R.E., Inclusion transformations: (n, m)-graphs and their classification, Discrete Mathematics 96 (1991) 111–129.

Several cominbatorial objects of general interest share similar definitions, i.e., complete bipartite graphs, Eulerian graphs and two-graphs. This article generalizes this definition to obtain a class of combinatorial objects known as (n, m)-graphs. A classification of (n, m)-graphs is presented that is complete for a big enough set of points. In the course of this classification, a theorem is proved that seems fundamental to the study of: the inclusion relation; (n, m)-graphs; certain sub-codes of the Reed–Muller codes and the irreducible representations of the symmetric group that arise from two-part partitions.

1. Introduction

Several combinatorial objects of general interest share a similar definition, i.e. complete bi-partite graphs, Eulerian graphs and two-graphs. This article generalizes this definition to obtain a class of combinatorial objects known as (n, m)-graphs. A classification of (n, m)-graphs is presented that is complete for a large enough set of points. In the course of this classification, a theorem is proved that seems fundamental to the study of (n, m)-graphs, sub-codes of the Reed–Muller codes [8] and the irreducible representations of the symmetric group that arise from two-part partitions [5]. The last example will be discussed in a later paper.

2. Definitions

We start with several well-studied combinatiorial objects with similar definitions. Throughout this paper, sets are finite and subsets are unordered. Let S be a set of size v and let an i-set of S be a subset of S which has size i. The following objects are defined:

(i) *Complete bi-partite graphs.* If S is a set and C is a set of 2-sets, C is a complete bi-partite graph if and only if every 3-set of S contains an even number of the elements of C.

(ii) *Eulerian graphs.* If S is a set and E is a set of 2-sets, E is a Eulerian graph if and only if every 1-set (or point) of S is contained in an even number of the elements of E.

(iii) *Two-graphs.* If S is a set and T is a set of 3-sets, T is a two-graph if and only if every 4-set of S contains an even number of the elements of T.

An immediate generalization is suggested by the above definitions:

(iv) *(n, m)-graphs.* If S is a set and D is a set of m-sets, D is an (n, m)-graph if and only if every n-set of S contains or is contained in an even number of the elements of D.

Notes: (i) (3, 2)-graphs, (1, 2)-graphs and (4, 3)-graphs correspond to complete bi-partite graphs, Eulerian graphs and two-graphs respectively.

(ii) Of the first three examples, two-graphs are probably the least well-known. They have proved applicable to various diverse areas of algebra and combinatorics [11], including permutation group theory, graph theory and Lie algebras.

(iii) The above definition of complete bi-partite graphs will be shown to be equivalent to the conventional definition. The reader is invited to check that conventionally defined complete bi-partite graphs have the (2, 1)-graph property.

(iv) Some authors would apply the additional constraint of being connected to the definition of a Eulerian graph.

(v) The (n, m)-graph definition has immediate connections with the theory of boolean functions. A function on v variables can be uniquely expressed as the sum (XOR) of products (ANDs) of subsets of the variables. The function is said to be of pure order m if every term in the function is the product of precisely m distinct variables. If $n > m$, we may enquire which functions of pure order m are identically zero when precisely n of the variables are nonzero. Such functions are identifiable with (n, m)-graphs, as described in Section 8.

(vi) $(k+1, k)$-graphs and $(k, k+1)$-graphs have been studied and analyzed by Cameron [2]. These cases will be shown to have a structure that is an extension of the general (n, m)-graph classification.

The next section introduces the key concept of realizability and exhibits a general class of (n, m)-graphs.

3. Realizability and a class of (n, m)-graphs

The concept of *realizability* is central to the classification of (n, m)-graphs: A set of t-sets T is said to *realize* a set of m-sets D if and only if D consists of the

m-sets of S that contain or are contained in an odd number of the elements of T. We say that D is *realized* by T or D is *t-realizable*.

T does not have to be unique in realizing D.

Examples. (i) The complete set of m-sets is realizable by the set containing the empty set (a 0-set).

(ii) A set of points P realizes the complete bi-partite graph between S and $S\backslash P$.

The last example is noteworthy as it illustrates that 1-realizability classifies (3, 2)-graphs. In fact, (4, 3)-graphs are 2-realizable and vice versa [11]. A substantial part of this article was derived generalizing these results.

The following results are elementary consequences of the definitions.

Lemma 3.1. (i) *The set-symmetric difference of two* (n, m)-graphs *is again an* (n, m)*-graph.*

(ii) *Two sets of t-sets realize the same set of m-sets if and only if their set-symmetric difference is an* (m, t)*-graph.*

(iii) *Suppose* $n > m > t$. *If* 2 *divides* $\binom{n-t}{m-t}$, *every t-realizable set of m-sets forms an* (n, m)*-graph.*

Proof. Let D_1 and D_2 be two sets of m-sets. Suppose that an n-set contains n_1 m-sets from D_1 and n_2 m-sets from D_2. Then, if the n-set contains n_3 elements in the set-symmetric difference of D_1 and D_2, $n_3 \equiv n_1 + n_2$ modulo 2. The first result follows as n_3 is even if both n_1 and n_2 are even. The second result follows by applying the result to (m, t) instead of (n, m), since n_3 is even if both n_1 and n_2 are odd. Let $T_d = \{\underline{d}\}$ where $\underline{d}$ is a t-set of S. For any n-set p of S, there are either 0 or $\binom{n-t}{m-t}$ m-sets j for which $\underline{d} \subseteq \underline{j} \subseteq \underline{p}$. If $\binom{n-t}{m-t}$ is even, it follows that T_d realizes a set of m-sets which is an (n, m)-graph. Since every set of t-sets is a set-symmetric difference of sets containing precisely one t-set, the third result follows. □

Lemma 3.1 supplies a general class of (n, m)-graphs when $m < n < |S|$. We define $T(p, n, m)$ and realizable (n, m)-graphs as follows:

$$\text{(i)} \quad T(p, n, m) = \begin{cases} \left\{ t \mid 0 \leq t < m,\ p \text{ divides } \binom{n-t}{m-t} \right\} & \text{if } p \neq 0, \\ \emptyset & \text{if } p = 0. \end{cases}$$

(ii) Let d be a set of m-sets of S. If D can be expressed as the set-symmetric difference of a number of t-realizable sets of m-sets, for varying values of t belonging to $T(2, n, m)$, then D is said to be a realizable (n, m)-graph.

Example ((5, 3)-*graphs*). For $n = 5$ and $m = 3$, $T(2, 5, 3) = \{0, 1\}$. If P is a set of points, the 3-sets realized by P consist of:

(i) The 3-sets of P;

(ii) The 3-sets containing precisely 1 point of P and 2 points of $S\backslash P$.
Note that these triples are indeed a $(5, 3)$-graph and that the addition of a 0-realizable set of points either leaves the 3-sets unchanged or takes the complimentary set of 3-sets. In the latter case, this is equivalent to swapping P for $S\backslash P$.

The main classification of (n, m)-graphs states that, provided $|S| \geq n + m > 2m$, every (n, m)-graph is realizable. This combinatorial result is best stated and proved as a linear algebra result.

4. Vector spaces and inclusion transformations

Let S be a set. For $m \leq |S|$, $P(m)$ is defined to be the set of all m-sets of S, i.e.,

$$P(m) = \{r \mid r \text{ is an } m\text{-set of } S\}.$$

If F is a field, $V(m, F)$ is defined to be the vector space over F which has the elements of $P(m)$ as a basis.

If $F = \mathrm{GF}(2)$, the nonzero coordinates of any vector of $V(m, F)$ can be used to identify the vector with a set of m-sets of S. Furthermore, vector space addition is identifiable with set-symmetric difference of the corresponding sets of m-sets.

The inclusion relation can be used to define a linear transformation between any two of the vector spaces defined over a common field. These transformations are given the generic title of inclusion transformations.

In more detail, let $m, n: 0 \leq m, n \leq v$. Define $A(m, n, F): V(m, F) \rightarrow V(n, F)$ by the action of $A(m, n, F)$ on the basis elements of $V(m, F)$,

$$r \cdot A(m, n, F) = \sum_{t \in P(n),\ r \subseteq t \text{ or } r \supseteq t} 1_F \cdot t, \quad \text{for all } r \in P(m).$$

Note that, if $F = \mathrm{GF}(2)$, the combinatorial definitions of the previous sections have a vector space interpretation. For example,

(i) If $v \in \ker A(n, m, F)$, then v is identified with an (n, m)-graph on S and vice versa;

(ii) The t-realizable sets of m-sets are identified with the vectors in $\operatorname{Im} A(t, m, F)$ and vice versa.

Lemma 3.1 has the following extension.

Lemma 4.1. (i) *If* $0 \leq t \leq m \leq n \leq v = |S|$, *then*

$$A(t, m, F) \cdot A(m, n, F) = \binom{n-t}{m-t}_F \cdot A(t, n, F)$$

(ii) If $\operatorname{char} F = p$, $0 < m < n \leq v$, *then*

$$\langle \operatorname{Im} A(t, m, F) \mid t \in T(p, n, m) \rangle \subseteq \ker A(m, n, F).$$

(iii) *If the dual space to* $V(m, F)$ *is identified with* $V(m, F)$ *using the dual basis, the annihilator of* $\ker A(m, n, F)$ (resp. $\operatorname{Im} A(m, n, F)$) *is identifiable with* $\operatorname{Im} A(n, m, F)$ (resp. $\ker A(n, m, F)$).

Proof. (i) By definition and the same counting argument as in Lemma 3.1.

(ii) Follows from (i).

(iii) A standard argument. See, for example, [1]. □

To work further with inclusion transformations, the following subspaces are fundamental: If $0 \leqslant j \leqslant m \leqslant n \leqslant |S|$,

(i) $R(j, m, F)$ is defined to be $\langle \operatorname{Im} A(i, m, F) \mid 0 \leqslant i \leqslant j \rangle$;

(ii) $\mathrm{PR}(j, m, n, F)$ is defined to be $\{v \mid v \in V(m, F),\ v \cdot A(m, n, F) \in R(j, n, F)\}$.

Notes. (i) $\mathrm{Pr}(j, m, n, F)$ and $R(j, m, F)$ are defined to be the zero subspace of $V(m, F)$ when $j < 0$.

(ii) For notational convenience, we will write $R(m, F)$ and $\mathrm{PR}(m, n, F)$ for $R(m-1, m, F)$ and $\mathrm{PR}(m-1, m, n, F)$ respectively.

(iii) By virtue of Lemma 3.1(i), $R(j, m, F) \subseteq \mathrm{PR}(j, m, n, F)$, as

$$w = \sum_{i=0}^{m} w(i) \cdot A(i, m, F) \text{ implies } w \cdot A(m, n, F) = \sum_{i=0}^{n} \binom{n-i}{m-i}_F w(i) \cdot A(i, n, F)$$

(iv) These subspaces have an intuitive interpretation in terms of boolean functions. This will be presented in Section 8.

(v) It will be shown in Part II of this paper that, if $|S| > 2m$, then $R(m, F)$ is the annihilator of the Specht module for the partition $(|S| - m, m)$.

We are now ready for the major theorem of this paper.

5. The Pre-Image Theorem and corollaries

Theorem 5.1 (Pre-Image Theorem). *If* $|S| \geqslant n + m$ *and* $n > m$, $\mathrm{PR}(m, n, F) = R(m, F)$.

Proof. See Appendix A. □

Notes. (i) The proof is by triple induction on $|S|$, m and n and appeared in [10].

(ii) The main idea behind the proof is to split the sets into those containing a point P and those that do not. This splits the action of $A(m, n, F)$ into that of inclusion transformations defined on $S \setminus P$. With a suitable inductive hypothesis, the theorem follows.

(iii) It is not generally true that $\mathrm{PR}(j, m, n, F) = R(j, m, F)$. However, it is possible to generalize Theorem 5.1 to give a classification of $\mathrm{PR}(j, m, n, F)$.

Because the results are not necessary for the rest of the paper, the details are relegated to Appendix B. The results and notation of Section 6 are used in that appendix.

(iv) It is possible to prove Theorem 5.1 by a maximal rank argument on the matrices induced by $A(m, n, F)$. However, the proof used in this paper is constructive: the same inductive steps can be used to generate basis elements for $R(m, F)$ and its dual. (This is exploited in Part II of the paper.) The author would like to thank an anonymous referee for pointing out the maximal rank approach was independently discovered by Wilson in unpublished work from about 1982–1983.

It remains to apply this theorem, establish the dimensions of all the defined subspaces and classify the structure of $\ker A(m, n, F)$ when $|S| \geqslant n+m$. Additonal notation is required.

(i) $T=\{T(i) \mid 0 \leqslant i \leqslant m\}$ is defined to be a co-space choice for $V(m, F)$ if $T(i)$ is a complementary subspace to $R(i, F)$, i.e., if

$$T=\{T(i) \mid 0 \leqslant i \leqslant m,\ T(i) \subseteq V(i, F),\ T(i)+R(i, F)=V(i, F),\ T(i) \cap R(i, F)=\emptyset\},$$

(ii) If $w \in V(m, F)$, then w is expressed in normal form with respect to T if and only if there exists a set $\{w(i) \mid 0 \leqslant i \leqslant m,\ w(i) \in T(i)\}$ for which

$$w=\sum_{i=0}^{m} w(i) \cdot A(i, m, F).$$

(iii) Whenever $0 \leqslant j<k$, $K(k, j, F)$ is defined to be

$$\bigcap_{i=0}^{j} \ker A(k, i, F).$$

(iv) $K(k, j, F)$ is defined to be $V(k, F)$ if $j<0$ and $K(k, k-1, F)$ is abbreviated as $K(k, F)$. ($K(k, F)$ is the principle focus of Part II of this paper. The subspace is isomorphic to the partition $[v-k, k]$.)

Corollary 5.2. *If $s=|S| \geqslant 2m-1$ and T is any co-space choice for $V(m, F)$, then*

(i) *Every element of $V(m, F)$ is uniquely expressible in normal form with respect to T.*

(ii) $\dim R(j, m, F)=\dim V(j, F)=\binom{s}{j}$, *when $j \leqslant m$.*

(iii) $\dim K(m, j, F)=\binom{s}{m}-\binom{s}{j}$, *when $j \leqslant m$.*

Proof. (i) Let $w \in V(m, F)$. Then there exist $t(m)$ and $r(m)$ for which $t(m) \in T(m)$, $r(m) \in R(m, F)$ and $w=t(m)+r(m)$. As $r(m) \in R(m, F)$, there exists $\{v(i) \mid 0 \leqslant i \leqslant m-1\}$ for which

$$r(m)=\sum_{i=0}^{m-1} v(i) \cdot A(i, m, F).$$

We now make the inductive hypothesis that for $i > j$, $v(i) \in T(i)$ and that the choice for the $v(i)$, $i > j$, is unique. We need to extend the induction to $i \geq j$. Suppose that $v(j)$ does not belong to $T(j)$. Let $v(j) = w(j) + r(j)$ where $w(j) \in T(j)$ and $r(j) \in R(j, F)$. Put

$$r(j) = \sum_{k=0}^{j-1} s(k) \cdot A(k, j, F).$$

Replace $v(d)$ by

$$u(d) = \begin{cases} v(d) & \text{if } d > j, \\ w(j) & \text{if } d = j, \\ v(d) + \binom{m-d}{j-d}_F \cdot s(d) & \text{if } d < j. \end{cases}$$

It follows that

$$w = \sum_{d=0}^{m-1} u(d) \cdot A(d, m, F) \quad \text{and} \quad u(d) \in T(d) \text{ for } d \geq j.$$

To close the induction, it is left to show that $u(j)$ is a unique choice. Assume that

$$w = \sum_{d=0}^{m-1} m(d) \cdot A(d, m, F) = \sum_{d=0}^{m-1} u(d) \cdot A(d, m, F),$$

where, by induction, $m(i) = u(i)$ for $i > j$ and $m(j) \in T(j)$. Given that

$$0 = \sum_{d=0}^{j} [m(d) - u(d)] \cdot A(d, m, F),$$

it follows that $[m(j) - u(j)] \in T(j) \cap \mathrm{PR}(j, m, F)$. As $|S| \geq 2m - 1 \geq m + j$, Theorem 5.1 states that $[m(j) - u(j)]$ belong to $T(j) \cap R(j, F)$ which, by definition of T, is the zero subspace. Hence $u(j)$ is equal to $m(j)$, the induction holds and (i) is proved.

(ii) The proof of (i) demonstrates that, as vector spaces,

$$V(j, F) \equiv \sum_{i=0}^{j} T(i) \equiv R(j, m, F), \quad \text{for all } j,\ 0 \leq j \leq m.$$

Thus, as $\dim V(j, F) = \binom{|S|}{j}$, (ii) is proved.

(iii) The annhilator of $K(m, j, F)$ is, by Lemma 4.1(iii), isomorphic to

$$\langle \operatorname{Im} A(i, m, F) \mid 0 \leq i < m \rangle = R(j, m, F).$$

Therefore

$$\begin{aligned} \dim K(m, j, F) &= \dim V(m, F) - \dim R(j, m, F). \\ &= \binom{|S|}{m} - \binom{|S|}{j}. \qquad \square \end{aligned}$$

We are now in a position to classify the kernels of inclusion transformations for $|S| \geq n+m \geq 2m$.

6. Kernels of inclusion transformations; classification of (n, m)-graphs

Theorem 5.1 and Corollary 5.2 allow the kernels of inclusion transformations to be described whenever the underlying set has sufficient points.

Theorem 6.1 (Realizability Theorem). *Provided $n > m$ and $|S| \geq n+m$, then*:
(i) *If* $\operatorname{char} F = 0$, $\ker A(m, n, F) = \underline{0}$.
(ii) *If* $\operatorname{char} F = p > 0$, $\ker A(m, n, F) = \langle \operatorname{Im} A(t, m, F) \mid t \in T(p, n, m) \rangle$.
In particular, if $T(p, n, m)$ is the empty set, $\ker A(m, n, F)$ *is* $\underline{0}$.

Proof. Let T be a co-space choice for $V(m, F)$ and $v \in \ker A(m, n, F)$. Then, as $v \cdot A(m, n, F) = \underline{0}$, $v \in \mathrm{PR}(m, n, F)$. As $|S| \geq n+m$, Theorem 5.1 states that $v \in R(m, F)$. Let

$$v = \sum_{i=0}^{j} v(i) \cdot A(i, m, F)$$

be the normal form expression for v. Thus,

$$v \cdot A(m, n, F) = \sum_{i=0}^{m-1} \binom{n-i}{m-i}_F \cdot A(i, n, F) = \underline{0}. \tag{1}$$

If j exists, maximal subject to $w(j) = \binom{n-j}{m-j}_F \cdot v(j)$ not being equal to $\underline{0}$, then it follows from (1) that

$$w(j) \in T(j) \cap \mathrm{PR}(j, n, F).$$

As $|S| \geq n+m > n+j$, Corollary 5.2 states that $w(j) = \underline{0}$, a contradiction. Thus $\binom{n-j}{m-j}_F \cdot v(j)$ is equal to $\underline{0}$ for all j, $0 \leq j \leq m-1$. This, by the definition of $T(p, n, m)$, proves the theorem. $\square$

Note that, if $\operatorname{char} F = 0$ or $T(p, m, m-1) = \emptyset$, $R(m, F) = \operatorname{Im} A(m-1, m, F) \equiv V(m-1, F)$.

Corollary 6.2. *Let m, n be such that $0 \leq m$, $n < |S| = s$.*
(a) *If* $\operatorname{char} F = 0$, *$A(m, n, F)$ has maximal rank.*
(b) *If* $\operatorname{char} F = p > 0$, *$s \geq n+m$ and $n > m$,*

$$\dim \ker A(m, n, F) = \sum_{t \in T(p, n, m)} \left[\binom{s}{t} - \binom{s}{t-1} \right].$$

(c) *If* char $F = p > 0$, $s < n + m$ *and* $n > m$,

$$\dim \ker A(m, n, F) = \binom{s}{m} - \binom{s}{n} + \dim \ker A(s - n, s - m, F).$$

(d) *If* char $F = p > 0$ *and* $n < m$,

$$\dim \ker A(m, n, F) = \dim \ker A(s - m, s - n, F).$$

(Note that $\dim \ker A(s - m, s - n, F)$ can be computed from case (a), (b) or (c).)

Proof. (a) is immediate from Theorem 6.1 and Corollary 5.2.

(b) Theorem 6.1 proved that, if $s \geqslant n + m$ and $n > m$, then, as vector spaces, $\ker A(m, n, F)$ is equal to the direct sum of the $T(i)$ for which $i \in T(p, n, m)$. As $\dim T(i) = \dim K(i, F)$, Corollary 5.2 proves case (b).

(d) Note that the map that takes x to $S \backslash x$, gives an obvious isomorphism of $V(m, F)$ to $V(s - m, F)$ that preserves inclusion, i.e., $a \subseteq b \rightarrow S \backslash a \supseteq S \backslash b$. It follows that $\dim \ker A(i, j, F) = \dim \ker A(s - i,\ s - j, F)$, proving case (d).

(c) We now use the dual basis result of Lemma 4.1.

$$\begin{aligned} \dim \ker A(m, n, F) &= \dim \ker A(s - m, s - n, F) \\ &= \binom{s}{m} - \dim \operatorname{Im} A(s - m, s - n, F) \\ &= \binom{s}{m} - \binom{s}{n} + \dim \ker A(s - m, s - n, F), \end{aligned}$$

by Lemma 4.1. This proves case (c) $\square$

Notes. (i) Kantor [6] proved Corollary 6.2(a) in a different setting.

(ii) In Theorem 5.1, bounds on the minimum size of $|S|$ appeared which were responsible for the $|S| \geqslant n + m$ bounds on the kernel of $A(m, n, F)$. A few numerical examples on the dimensions should persuade the reader of the necessity for this bound. Specific counterexamples to a 'boundless Theorem 6.1' will be exhibited in Section 7.

The Theorem 6.1 condition $|S| \geqslant 2m + 1$ can be removed for the special case of the $(m + 1, m)$-graphs.

Theorem 6.3. *If* char $F = 2$ *and* $|S| \geqslant m + 1$, *then*

$$\ker A(m, m + 1, F) = \operatorname{Im} A(m - 1, m, F).$$

In particular, every $(m + 1, m)$*-graph is* $(m - 1)$*-realizable.*

Proof (*from* [2]). Let $v = \sum_{t \in P(m)} a(t) \cdot t$ belong to $\ker A(m-1, m, F)$ and let Q be a point of S. Define $w(v) \in V(m-1, F)$ by

$$w(v) = \sum_{s:\, Q \in s \in P(m)} a(s) \cdot [s \backslash Q].$$

Then, as $v \in \ker A(m, m+1, F)$ and $\operatorname{char} F = 2$, $w(v) \cdot A(m-1, m, F) = v$. $\square$

Notes. (i) If $|S| \geqslant 2m+1$, the above result is consistent with Theorem 6.1 as

$$T(2, m+1, m) = \{t \mid m+1-t \text{ is even, } 0 \leqslant t < m\},$$

$$A(t, m-1, F) \cdot A(m-1, m, F) = (m-t)_F \cdot A(t, m, F) \quad \text{and}$$

$$\langle \operatorname{Im} A(t, m-1, F) \mid t \in T(2, m+1, m, F) \rangle = \operatorname{Im} A(m-1, m, F).$$

(ii) It can be shown that Theorem 6.3 is dimensionally consistent with Theorem 6.2.

(iii) Theorem 6.3 creates an interesting chain structure for $(m+1, m)$-graphs: Every $(m+1, m)$-graph is $(m-1)$-realizable by a set of $(m-1)$-sets; Two sets of $(m-1)$-sets realize the same $(m+1, m)$-graph if and only if their set-symmetric difference is a $(m, m-1)$-graph; Every $(m, m-1)$-graph is $(m-2)$-realizable by a set of $(m-2)$-sets, etc.

(iv) We have verified the classification of complete bi-partite graphs used in Section 2; 1-realizable graphs are equivalent to $(3, 2)$-graphs. Moreover, if two graphs realize the same two-graph, their set-symmetric difference of edge sets form a complete bi-partite graph. Two graphs are said to be in the same *switching class* of graphs if the set-symmetric difference of their edge sets is an edge set for a complete bi-partite graph. It follows that switching classes of graphs are matched to $(4, 3)$-graphs [11, 7], in that a switching class of graphs realize the same $(4, 3)$-graph and a $(4, 3)$-graph is realized by a unique switching class. (The correspondence also respects the action of the symmetric group [7].)

The next section gives some specific examples of the Realizability Theorem.

7. Examples and classifications of some (n, m)-graphs

The following theorems will be needed.

Theorem 7.1 (Lucas). *Let p be a prime and k a positive integer. Write $k = \sum_{i \geqslant 0} a(i, k) p^i$, with $0 \leqslant a(i, k) < p$, the expansion of k in base p. Then*

$$\binom{k}{d} = \prod_{i \geqslant j} \binom{a(i, k)}{a(i, d)} \text{ modulo } p, \quad \text{where } \binom{f}{e} = 0, \text{ if } e > f.$$

A proof can be found in Dickson [3].

Theorem 7.2 (Reducibility Theorem). *Let p be a prime. If $m>0$, let t be the integer for which*

$$p^t \leq m < p^{t+1}.$$

If $n \geq m$, define r to be that number between m and $m+p^{t+1}$-1 for which

$$n \equiv r \text{ modulo } p^{t+1}.$$

Then $T(p,n,m) = T(p,r,m)$. In particular, if $|S| \geq n+m$, every (n,m)-graph on S is also an (r,m)-graph on S.

Proof. A straightforward application [10] of Lucas' Theorem. □

Thus, for example, if $|S| \geq 468$, every $(465, 3)$-graph on S is also a $(5, 3)$-graph.

Examples. (a) *$(n, 2)$-graphs on S.*

(i) $(3,2)$-graphs on S. by Theorem 6.3, all $(3,2)$-graphs are 1-realizable, i.e, the $(3,2)$-graphs are the edge sets of complete bi-partite graphs.

(ii) $(4,2)$-graphs on S. $|S| \geq 6$; by Theorem 6.1, if D is a $(4,2)$-graph on S, D is 0-realizable, i.e., D is either the complete or empty set of 2-sets. This result can not be strengthened. If $|S|| = 5$, then the graph in Fig. 1 has an edge set which is a $(4,2)$-graph but not 0-realizable.

(iii) $(5,2)$-graphs on S. $|S| \geq 7$; $T(2,5,2) = \{0, 1\}$. Hence, if D is a $(5,2)$-graph on S, then D is either the edge set of a complete bi-partite graph or the disjoint union of two complete graphs.

(iv) $(6,2)$-graphs on S. $|S| \geq 8$; $T(2,6,2) = \emptyset$ and the only $(6,2)$-graph on S is the empty set of 2-sets.

(v) $(n,2)$-graphs on S. $|S| \geq n+2$; by Theorem 7.2, these are $(m,2)$-graphs where $3 \leq m \leq 6$ and m is congruent to n modulo 4.

(b) *$(n, 3)$-graphs on S.*

(i) $(4,3)$-graphs on S. by Theorem 6.3, every $(4,3)$-graph is 2-realizable and, as described above, the $(4,3)$-graphs are in correspondence with switching classes of graphs.

(ii) $(5,3)$-graphs on S. $|S| \geq 8$; $T(2,5,3) = \{0, 1\}$ and the complete set of triples are 1-realizable as well as 0-realizable $(A(0,1,F) \cdot A(1,3,F) = A(0,3,F))$. Moreover, the only $(3,1)$-graph on S is the empty set of points. It

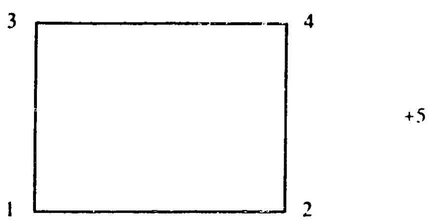

Fig. 1. A $(4,2)$-graph that is not 0-realizable.

follows that, if $|S| \leq 8$, $(5, 3)$-graphs on S are in 1–1 correspondence with the subsets of S, i.e., there are $|S| + 1$ non-isomorphic $(5, 3)$-graphs on S. If $|S| < 8$, this is not true. There are (see [9]) 56 non-isomorphic $(5, 3)$-graphs on S if $|S| = 7$. For example, the lines of the 2-(7, 3, 1) projective plane [4] of order 2 form a nonrealizable $(5, 3)$-graph on 7 points which has the minimum cardinality of any $(5, 3)$-graph on 7 points.

(iii) $(6, 3)$-graphs on S. $|S| \geq 9$; $T(2, 6, 3) = \{0, 1, 2\}$ and $\ker A(3, 6, F) = R(3, F)$. Hence any $(6, 3)$-graph on S can be described as the set-symmetric difference of a $(4, 3)$-graph and a $(5, 3)$-graph.

(iv) $(7, 3)$-graphs on S. $|S| \geq 10$; $T(2, 7, 3) = \emptyset$ and no non-empty $(7, 3)$-graph on S exists.

(v) $(n, 3)$-graphs on S. $|S| \geq n + 3$, $n > 7$; by reducibility, these are just $(m, 3)$-graphs where $4 \leq m \leq 7$ and m is equal to n modulo 4.

8. Partial truth table interpretation of inclusion transformations

A boolean function on v variables is defined as the binary sum of multiples of subsets of $x_1, x_2, \ldots, x_v$. For example consider the example of $v = 4$ and the function

$$f(x_1, x_2, x_3, x_4) = 1 + x_3 + x_1 + x_4 \cdot x_3 + x_4 \cdot x_1.$$

We say that a function is of order r if the maximum number of multiplied x_i is r, e.g., the above function is of order 2. A function is of pure order r if every term is of order r. In the inclusion transformation approach the terms are replaced by subsets. For example, the above function becomes

$$f = 1 \cdot \emptyset + 1 \cdot \{3\} + 1 \cdot \{1\} + 1 \cdot \{3, 4\} + 1 \cdot \{4, 1\}.$$

Notes. (i) Any function can be split into a sum of functions of pure order.

(ii) $V(i, F)$, $F = \mathrm{GF}(2)$, can be identified with the functions of pure order i, i.e., $V(i, F)$ is spanned by the subsets of size i.

We now consider the process of evaluating a function at an input. Let the input be $\underline{t} = (t_1, t_2, t_3, \ldots, t_v)$. We may consider $\underline{t}$ to be a subset of size i where i is equal to the binary Hamming weight of $\underline{t}$. For example, $\underline{t} = (0111)$ can be identified with $\{2, 3, 4\}$. With this identification, evaluation of a function becomes identified with the inclusion relation. For example, evaluating the example function at (0111) is identical to taking the set $\{2, 3, 4\}$ and considering if an odd or even number of the elements $\emptyset$, $\{3\}$, $\{1\}$, $\{3, 4\}$ and $\{1, 4\}$ are contained in $\{2, 3, 4\}$. In fact, there are three such contained elements and the function is equal to 1 at this point. We write $f(\{a, b, c\})$ for the evaluation of f at the $\underline{t}$ that corresponds to the subset $\{a, b, c\}$. If we evaluated the function at all the inputs of weight 3, we would end with a vector $v_{f,3}$ in $V(3, F)$,

$$v_{f,3} = \sum_{\{a,b,c\}} f(\{a, b, c\}) \cdot \{a, b, c\}.$$

It should be apparent that the process of evaluating a pure function of order i on the inputs of weight j is identical to applying $A(i, j, F)$ to the corresponding vector in $V(i, F)$, where $F = \mathrm{GF}(2)$ and $j \geqslant i$. In functional terms, a function of pure order m corresponds to an (n, m)-graph if and only if the function is equal to zero for every input of weight n. It follows that, provided the number of variables exceeds $n + m$, Section 6 has classified such functions and Section 7 presents examples for $m = 2$ and 3.

Note that we now have a duality in our interpretation of a vector in $V(i, F)$. In one interpretation, this is a function of pure order i. In another interpretation this is the set of outputs for a function evaluated on all the inputs of binary weight i. In fact, this duality allows a more interpretative view of $R(m, F)$; $R(m, F)$ is the subspace in $V(m, F)$ of partial truth tables for functions of degree lower than m. $A(m, n, F)$ can be thought of as the connection between the view of a vector in $V(m, F)$ as either a function of pure order m or a partial truth table. This duality allows us to restate Theorem 6.1. We assume that $v \geqslant r + k \geqslant r > k$. Then the following holds.

> If a function f of pure order k is evaluated on all the inputs of weight r and the resulting partial truth table is identical to that obtained from a function of order lower than k, then f is itself the partial truth table for a function of order lower than k.

Appendix B generalizes Theorem 5.1 and, as a corollary, we get a tighter result than the above. We define $S(2, n, m, j)$ to be the maximum of j and the elements of $T(2, n, m)$. We assume that $v \geqslant r + k \geqslant r > k > j$. Then we have the following.

> If a function f of pure order k is evaluated on all the inputs of weight r and the resulting partial truth table is identical to that obtained from a function of order j, then f is the partial truth table for a function of order at most $S(2, n, m, j)$.

There is a close connection between these subspaces and the Reed–Muller codes. These codes are defined by taking a binary code on v variables and substituting the truth table for f, i.e., the evaluations of the function f at all the possible subsets. If we consider the entire truth table for a function of order r to be the sum of the partial truth tables for $V(i)$, $0 \leqslant i \leqslant |S|$, we get an important class of punctured subcodes of the Reed–Muller codes: $R(r, k, F)$ is the sub-space of $V(k, F)$ that consists of the vectors that are the partial truth tables for functions of order r evaluated at the inputs of weight k.

9. Conclusions

This completes the fundamental definitions and classification for (n, m)-graphs. The paper has identified certain subspaces, namely $R(m, F)$ and $\mathrm{PR}(k, m, F)$, which are basic in studying these objects. A fundamental theorem identifying these subspaces has allowed a structure for the kernel of the inclusion transformations to be deduced. The same results and classification can be re-interpreted in the field of boolean functions. In fact, the clearest statement of Theorem 6.1 is probably in this language. Throughout the article little use has been made of the invariance of the subspaces under the action of the symmetric group. A second article will report on this aspect.

Appendix A: Proof of Theorem 5.1

The central idea of the proof is to examine the effect of a point $Q \in S$ on the inclusion transformations. In order to obtain an inductive proof of Theorem 5.1, we need some notation.

We will write $V(k, S, F)$ for $V(k, F)$ defined on the set S, i.e., the basis for $V(k, S, F)$ is the set of k-sets of S. Similarly, $P(k, S)$ is the set of all k-sets of S, $A(m, n, S, F)$ is the inclusion transformation $A(m, n, F)$ defined on the set S and similarly for $R(j, m, S, F)$ etc.

Let k, $0 \leqslant k \leqslant |S|$, $w \in V(k, S, F)$ and $Q \in S$. We split w into the sum of two vectors where the vectors are defined by the inclusion or otherwise by Q. Let

$$w = \sum_{t \in P(k, S)} w_t \cdot t.$$

Then $w = \bar{w} + \underline{w}$, where,

(i) $$\bar{w} = \sum_{t \in P(k, S)} \bar{w}_t \cdot t, \quad \text{and} \quad \bar{w}_t = \begin{cases} w_t & \text{if } Q \in t, \\ 0_F & \text{otherwise,} \end{cases}$$

(ii) $$\underline{w} = \sum_{t \in P(k, S)} \underline{w}_t . t, \quad \text{and} \quad \underline{w}_t = \begin{cases} 0_F & \text{if } Q \in t, \\ w_t & \text{otherwise.} \end{cases}$$

This vector splitting produces two subspaces:

(i) $J(k, S, F) = \{\bar{w} \mid w \in V(k, S, F)\}$,

(ii) $D(k, S, F) = \{\underline{w} \mid w \in V(k, S, F)\}$.

It follows that $V(k, S, F)$ is the direct sum of $J(k, S, F)$ and $D(k, S, F)$. In fact, $D(k, S, F)$ is isomorphic to $V(k, S \backslash Q, F)$ and $J(k, S, F)$ is isomorphic to $V(k-1, S \backslash Q, f)$. The first isomorphism follows by identifying the vector

$$\underline{w} = \sum_{t \in P(k, S)} \underline{w}_t \cdot t \quad \text{of } D(k, S, F)$$

with the vector

$$\underline{w}^{\mathrm{id}} = \sum_{r \in P(k,\, S \setminus Q)} w_r \cdot r \quad \text{of } V(k, S\setminus Q, F).$$

Isomorphisms between $J(k, S, F)$ and $V(k-1, S\setminus Q, F)$ are defined by inserting and deleting Q from various basis elements. In more detail, let $k > 1$ and $\bar{w} \in J(k, s, F)$. Let

$$\bar{w} = \sum_{t:\, Q \in t \in P(k,\, S)} w_t \cdot t + \sum_{r \in P(k,\, S),\, Q \notin r} 0_F \cdot r.$$

We now define $\bar{w}^Q \in V(k-1, S\setminus Q, F)$ by

$$\bar{w}^Q = \sum_{t:\, Q \in t \in P(k,\, S)} w_t\{t \setminus Q\}.$$

Analogously, if

$$y \in V(k-1, S\setminus Q, F)$$

and

$$y = \sum_{s \in P(k-1,\, S\setminus Q)} c_s \cdot s,$$

define $y^{\mathrm{I}} \in J(k, S, F)$, by

$$y^{\mathrm{I}} = \sum_{s \in P(k-1,\, S\setminus Q)} c_s[s \cup Q] + \sum_{t \in P(k,\, S\setminus Q)} 0_F \cdot t.$$

From definition.

$$(\bar{w}^Q)^{\mathrm{I}} = \bar{w}.$$

These operations define isomorphisms for $k > 1$:

(i) The map α_k is defined to go from $J(k, S, F)$ to $V(k-1, S\setminus Q, F)$ where $\alpha_k(\bar{w}) = \bar{w}^Q$

(ii) The map β_k is defined to go from $V(k-1, S\setminus Q, F)$ to $J(k, S, F)$ where $\beta_k(y) = y^{\mathrm{I}}$

From the above, α_k is an isomorphism of $J(k, S, F)$ to $V(k-1, S\setminus Q, F)$ and β_k is the inverse map.

The point of defining these subspaces and maps lies in their interaction with inclusion transformations. These interactions are summarized in the following lemma.

Lemma A.1. *If* $w \in V(k, S, F)$ *and* $1 \leq k < d \leq |S|$, *then,*

(a) $\quad \bar{w} \cdot A(k, d, S, F) = [\bar{w}^Q \cdot A(k-1, d-1, S\setminus Q, F)]^{\mathrm{I}}$.

Alternatively, when restricted to $J(k, s, F)$,

$$A(k, d, S, F) = \alpha_k \cdot A(k-1, d-1, S\setminus Q, F) \cdot \beta_d,$$

where the maps on the right hand side of the equation are applied in a left to right order.

(b) $\underline{w} \cdot A(k, d, S, F) = \underline{w} \cdot A(k, d, S\backslash Q, F) + [\underline{w} \cdot A(k, d-1, S\backslash Q, F)]^1$.

Proof. The inclusion transformations are defined by the action on the basis elements. Consider the action of $A(k, d, S, F)$ on $1_F \cdot s$, where s is a subset of size k that contains Q. If t is any d-set that contains s, it follows that $t\backslash Q \supseteq s\backslash Q$. This proves A.1(a).

Similarly, if r is a k-set of S that does not contain Q, i.e., $r \in P(k, S\backslash Q)$, and t is any d-set of S that contains r, then if $Q \in t$ it follows that $s\backslash Q \supseteq r$. This proves A.1(b). We are now in a position to prove Theorem 5.1. The theorem can be stated as follows.

Theorem A.2 (Pre-Image Theorem). *If* $|S| \geq n+m$ *and* $n > m$,

$$\mathrm{PR}(m-1, m, n, S, F) = R(m-1, S, F).$$

Proof. The proof will be by induction. Note that, if $m = 0$, there is nothing to prove.

Stage 1: $\mathrm{PR}(0, 1, n, S, F) = R(0, 1, S, F)$, *if* $|S| \geq n+1$.

Let $v \in \mathrm{PR}(0, 1, n, S, F) \subseteq V(1, S, F)$. By definition, there exists $a \in F$ for which

$$v \cdot A(1, n, S, F) = [a \cdot \emptyset] \cdot A(0, n, S, F) = \sum_{t \in P(m, S)} a \cdot t.$$

If we expand v into

$$v = \sum_{Q \in S} a_Q \cdot Q,$$

it follows that, for any $t \in P(n, S, F)$, $\sum_{Q \in t} a_Q = a$, i.e., the summation over a n-set is constant. Note that, if R and T are any two distinct points of S, as $|S| \geq n+1$, there exists an $(n-1)$-set h for which $r_1 = h \cup \{R\}$ and $r_2 = h \cup \{T\}$ are two distinct n-sets of S. Applying the constant sum property to r_1 and r_2 we conclude that a_T is equal to a_R and, in general, a_T is a constant independent of T. Put $b = a_T$ and we see that

$$v = b \cdot \left[\sum_{T \in P(1, S)} 1_F \cdot T\right] = [b \cdot \emptyset] \cdot A(0, 1, S, F),$$

i.e., $v \in R(0, 1, S, F)$, proving Stage 1.

Given this starting condition, it is possible to make an inductive hypothesis.

Hypothesis. The hypothesis is in two parts:

(A) $\mathrm{PR}(k, m, S, F) = R(k, S, F)$ provided (1) $|S| \geq m+k$, and (2) $1 \leq m < r$.

(B) $\mathrm{PR}(k, r, S, F) = R(k, S, F)$ provided (1) $|S| \geq k+r$, and (2) $1 \leq k < e$.

It remains to prove that, if $|S| \geqslant e+r$, $\mathrm{PR}(e, r, S, F) = R(e, S, F)$. Let $v \in \mathrm{Pr}(e, r, S, F)$ and $|S| \geqslant e+r$. Put

$$v \cdot A(e, r, S, F) = \sum_{j=0}^{j=e-1} v_j \cdot A(j, r, S, F) \tag{a}$$

Stage 2: *If* $v \in J(e, S, F)$, *then* $v \in R(e, S, F)$.
By definition, $v \in J(e, S, F)$ if and only if $v = \bar{v}$. Expanding equation (a) gives

$$\bar{v} \cdot A(e, r, S, F) = \sum_{j=1}^{e-1} \bar{v}_j \cdot A(j, r, S, F) + \sum_{j=0}^{e-1} \underline{v}_j \cdot A(j, r, S, F).$$

By Lemma A.1, this states that

$$\begin{aligned}[\bar{v}^Q \cdot A(e-1, r-1, S\backslash Q, F)]^{\mathrm{I}} = {} & \left[\sum_{j=1}^{e-1} \bar{v}_j^Q \cdot A(j-1, r-1, S\backslash Q, F)\right]^{\mathrm{I}} \\ & + \left[\sum_{j=0}^{e-1} \underline{v}_j \cdot A(j, r-1, S\backslash Q, F)\right]^{\mathrm{I}} \\ & + \sum_{j=0}^{e-1} \underline{v}_j \cdot A(j, r, S\backslash Q, F).\end{aligned}$$

It follows that

$$\sum_{j=0}^{e-1} \underline{v}_j \cdot A(j, r, S\backslash Q, F) = \underline{0}, \tag{A1}$$

$$\begin{aligned}\bar{v}^Q \cdot A(e-1, r-1, S\backslash Q, F) = {} & \sum_{j=1}^{e-1} \bar{v}_j^Q \cdot A(j-1, r-1, S\backslash Q, F) \\ & + \sum_{j=0}^{e-1} \underline{v}_j \cdot A(J, r-1, S\backslash Q, F).\end{aligned} \tag{A2}$$

Equation (A1) states that $\underline{v}_{e-1} \in \mathrm{PR}(e-1, r, S\backslash Q, F)$. As $|S\backslash Q| \geqslant e+r-1 > (e-1)+r$, part (B) of the induction hypothesis states that $\underline{v}_{e-1} \in R(e-1, S\backslash Q, F)$.

Equation (A2) states that $\bar{v}^Q - \underline{v}_{e-1} \in \mathrm{PR}(e-1, r-1, S\backslash Q, F)$. As $|S\backslash Q| \geqslant e+r-1 > (e-1)+(r-1)$, part (A) of the induction hypothesis states that $\bar{v}^Q - v_{e-1} \in R(e-1, S\backslash Q, F)$.

Hence, putting these two conclusions together, $\bar{v}^Q \in R(e-1, S\backslash Q, F)$. Let $\{y_j \mid 0 \leqslant j \leqslant e-2\}$ be such that

$$\bar{v}^Q = \sum_{j=0}^{e-2} y_j \,.\, A(j, e-1, S\backslash Q, F).$$

Then, by Lemma A.1,

$$\bar{v} = (\bar{v}^Q)^{\mathrm{I}} = \sum_{j=0}^{e-2} y_j^{\mathrm{I}} \cdot A(j+1, e, S\backslash Q, F).$$

Hence $v = \bar{v} \in R(e, S, F)$ and Stage 2 is proved.

Stage 3: $v \in \mathrm{PR}(e, r, S, F)$.

If $z = v \cdot A(e, r, S, F) = \sum_{j=0}^{e-1} v_j \cdot A(j, r, S, F)$, then Lemma A.1 states that

$$\bar{z} = \bar{v} \cdot A(e, r, S, F) + [\underline{v} \cdot A(e, r-1, S\backslash Q, F)]^{\mathrm{I}}$$
$$= \sum_{j=0}^{e-1} \bar{v}_j \cdot A(j, r, S, F) + \left[\sum_{j=0}^{e-1} \underline{v}_j \cdot A(j, r-1, S\backslash Q, F)\right]^{\mathrm{I}}.$$

Hence, using Lemma A.1 again,

$$\bar{v}^Q \cdot A(e-1, r-1, S\backslash Q, F) + \underline{v} \cdot A(e, r-1, S\backslash Q, F)$$
$$= \sum_{j=1}^{e-1} \bar{v}_j^Q \cdot A(j-1, r-1, S\backslash Q, F) + \sum_{j=0}^{e-1} \underline{v}_j \cdot A(j, r-1, S\backslash Q, F).$$

It follows that $\underline{v} \in \mathrm{PR}(e, r-1, S\backslash Q, F)$. As $|S\backslash Q| \geqslant e + r - 1 = e + (r-1)$, part (A) of the inductive hypothesis states that $\underline{v} \in R(e, S\backslash Q, F)$. Let

$$\{f_j \mid 0 \leqslant j \leqslant e-1, f_j \in V(j, S\backslash Q, F)\}$$

be such that $\underline{v} = \sum_{j=0}^{e-1} f_j \cdot A(j, e, S\backslash Q, F)$. We now regard each f_j as a vector in $V(j, S, F)$ and put

$$w = \sum_{j=0}^{e-1} f_j \cdot A(j, w, S, F).$$

Note that:

(i) $w \in R(e, S, F) \subseteq \mathrm{PR}(e, r, S, F)$.

(ii) $\underline{w} = \underline{v}$.

(iii) $v - w \in \mathrm{PR}(e, r, S, F)$ and $v - w \in J(e, S, F)$.

Thus, by Stage 2, $v - w \in R(e, S, F)$ and so $v \in R(e, S, F)$, proving the theorem. $\square$

Appendix B: A generalization of Theorem 5.1

Theorem 5.1 proved that $\mathrm{PR}(m-1, m, n, F) = R(m-1, m, F)$ when $|S| \geqslant n + m$. It is fairly immediate to see that, in general, $\mathrm{PR}(j, m, n, F) \neq R(j, m, F)$. For example, if this was the case and $v \in \ker A(m, n, F)$ this would imply that $v \in \mathrm{PR}(0, m, n, F)$ and, consequently, v would belong to $R(0, m, F)$, i.e., v would be the empty or complete sets of m-sets. Since this is not necessarily true, $R(j, m, F)$ may be a proper subset of $\mathrm{Pr}(j, m, n, F)$. However, it is not difficult to characterize $\mathrm{PR}(j, m, F)$.

Theorem B.1. *If* $|S| \geqslant n + m$ *and* $n > m > j$, *then*:

(i) $\mathrm{PR}(j, m, n, F) = \langle \ker A(m, n, F), R(j, m, F) \rangle$,

(ii) $\mathrm{PR}(m, n, F) = R(j, m, F)$ *if and only if* $T(p, n, m) \subseteq \{i \mid 0 \leqslant i \leqslant j\}$, *where* $\mathrm{char}\, F = p$.

Proof. Let $v \in \mathrm{PR}(j, m, n, F)$. Then, by Theorem 5.1, $v \in R(m-1, m, F)$. We write v and $v \cdot A(m, n, F)$ in normal form with respect to a co-space choice T,

$$v = \sum_{i=0}^{m-1} t_i \cdot A(i, m, F), \quad \text{where } t_i \in T(i), \tag{1}$$

As v is a member of $\mathrm{PR}(j, m, n, F)$, we know that

$$v \cdot A(m, n, F) = \sum_{i=0}^{j} p_k \cdot A(k, n, F), \quad \text{where } p_k \in T(k), \tag{2}$$

Applying $A(m, n)$ to equation (1) gives

$$\sum_{i=0}^{m-1} \binom{n-i}{m-i}_F t_i \cdot A(i, n, F) = \sum_{i=0}^{j} p_k \cdot A(k, n, F).$$

As in the proof of 5.2(i) and 6.1, we may apply Theorem 5.1 to conclude

$$\binom{n-i}{m-i}_F t_i = \begin{cases} 0 & \text{if } i > j, \\ p_i & \text{otherwise,} \end{cases}$$

proving the theorem. □

Notes. (i) The proof is slightly stronger than the statement of the theorem; a method is demonstrated of transferring the coefficients from $\mathrm{PR}(j, m, n, F)$ into part of $R(j, m, F)$.

(ii) The second condition gives a number-theoretic condition for the containment.

References

[1] E. Artin, Geometric Algebra (Wiley, New York, 1988).
[2] P.J. Cameron, Cohomological aspects of two-graphs, Math. Z. 157 (1977) 101–119.
[3] L.E. Dickson, Theory of Numbers, Vol. 1 (Chelsea, New York, 1952).
[4] D.R. Hughes and F.C. Piper, Projective Planes (Springer, Berlin, 1973).
[5] G.D. James, The Representation Theory of the Symmetric Groups (Springer, Berlin, 1978).
[6] W.M. Kantor, On incidence matrices of finite projective and affine spaces, Math. Z. 124 (1972) 315–318.
[7] C.L. Mallows and N.J.A. Sloane, Two-graphs, switching classes and Euler graphs are equal in number, SIAM J. Appl. Math. 28 1975 876–880.
[8] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes (North-Holland, Amsterdam, 1977).
[9] R.E. Peile, Combinatorial systems, M.Sc. Dissertation, Oxon, 1977.
[10] R.E. Peile, Some topics in combinatorial theory, Ph.D. Thesis, Oxon, 1979.
[11] J.J. Seidel, A survey of two-graphs, Colloq. Internaz. sulle Teorie Combinateorie, Roma, Accademia Nazionale dei Lincie, 1976.